REMARKS

1. Applicant thanks the Examiner for the Examiner's comments, which have greatly assisted Applicant in responding.

35 U.S.C. §103

3. Claims 1-40 are rejected by the Examiner under 35 U.S.C. §103(a) as being unpatentable over Vaid et al U.S. Patent No. 6,502,131 (hereinafter Vaid) in view of Rogers et al U.S. Patent No. 5,557,747 (hereinafter Rogers).

Applicant respectfully disagrees. Applicant is of the opinion that a prima facie case of obviousness was not established because the three basic criteria were not met. Specifically and at least, the prior art of reference do not teach all the claim limitations. Support follows hereinbelow.

(a) Claim 1 (and 13)

First, Applicant has amended Claim 1 (13) including incorporating some limitations from Claims 2 (14) and 5 (17) and relying on pages 17, line 9, through page 20, line 5 of the Specification to further clarify the invention. Amended Claim 1 appears as follows:

> 1. (currently amended) A system for analyzing network traffic to use in performing network and security assessments by listening on a subject network, interpreting events, and taking action, comprising:
>
> a policy specification file;
>
> a network monitor processor ~~for processing~~ that processes network packet data collected from said subject network; and
>
> a policy monitoring component ~~for receiving and processing~~ that receives and processes said policy specification file[[,]] and that receives and processes ~~receiving and processing~~ said processed network packet data to assign policy dispositions to network events contained in said network packet data, wherein said policy monitoring component further comprises a policy engine that:
>
> as each network packet arrives, compares said network packet data against said policy specification file and responsive to said comparison assigns

associated policy dispositions and level of severity to said network events contained in said network packet data;

interprets each protocol event; and

consults said policy specification file as each protocol event is interpreted to ensure that an earliest determination of said disposition is reached.

Regarding the limitation in original Claim 2, a policy engine... for performing the assign dispositions and level of severity to the network events contained in the network packet data, and other items, the Examiner cited Vaid, col. 14:6-32 and 16:55-17:56.

Applicant respectfully points out that regarding [14:6-32], all that it describes is a "security policy provides parameters for securing the present tool." Also, "the present tool can be configured based upon at least the following components – traffic classes, traffic policies, traffic rules, and traffic entities."

Then, [16:55-17:56] teaches the following (emphasis added):

> **The present method occurs at start, which is step 801, for example. In general, a flow of information or data or packets of information enter a gateway point, where the present tool sits.** The present method classifies (step 803) the flow of information. Groups of flows can be referred to as traffic classes, but are not limited to such classes. Classes also can be defined by source, destination, application, file types, URLs, and other features. Other examples of classes were previously noted, but are not limited to these classes. In general, step 803 classifies the flow of information received into one of a plurality of predetermined classes.
>
> The present tool measures parameters for each of the classes in step 805, which were received, for example. These parameters are based upon the policy or rule, **which may be applied in a later step**. As merely an example, parameters include the class itself, file sizes, and other information, which can be used by the policy or rule to apply the policy or rule to improve the quality of service for the network. After measuring the parameters, the present method applies a time stamp (step 807) on the parameters to correlate the class of information received to a time, for example.

> **A step of determining whether to apply a policy occurs in the next step 809**. For example, if the class and the time (and the link state in some embodiments) meet predetermined settings, the policy is applied to the class in step 811 through branch 810. Alternatively, if one of the elements including the class, the time, or the link state do not meet the predetermined settings, the policy does not apply and the process continues to measure parameters through branch 808. Alternatively, the process continues to measure parameters through branch 813 after the policy is applied to the flow of information for the class.

It is evident that Vaid **teaches away** from the claimed invention, because it teaches determining whether or not to apply a policy.

In stark contrast, the policy engine of the claimed invention compares said processed network packet data against said policy specification file and responsive to said comparison assigns associated policy dispositions and level of severity to said network events contained in said network packet data.

Furthermore, the policy engine of the claimed invention interprets protocol events from the network packet and, is capable of assigning a disposition to the network event based on a discovery of a protocol event, as follows (see Specification page 19, lines 7-17, emphasis added):

> The default action of the policy engine 102 is that it denies all traffic. The policy 105 opens holes in this denial to allow permitted traffic to flow. **Although the policy engine 102 assigns a single disposition to an entire network event, the protocol events are significant. As network data 115 arrives, the policy engine 102 interprets protocols** and generates updates of protocol event information. **The policy 105 is consulted as each new piece of information arrives, so that the earliest determination of disposition is reached.** For example, if the policy 105 states that a given IP address may not communicate with another IP address, the policy 105 can generate a disposition immediately upon receiving the first packet 115 of the network event.

This above limitation is claimed in original Claim 5 (17), which have been canceled without prejudice and are incorporated into independent Claim 1 (13). The Examiner stated that Vaid covers the limitations of Claim 5 and cited Figure 2, References No.

231 and related text. First, Applicant respectfully requests that the Examiner make clear his rejection by citing the actual steps, elements, or paragraphs, because to state "and related text" is ambiguous. The burden should not be on Applicant to interpret what the Examiner is using to cite against the claimed invention. See

However, in the spirit of compact prosecution, Applicant responds by Figure 2, No. 231 shows a schematic block of a policy engine module comprising: a security policy, traffic policy, and other. However, nowhere does Vaid teach as each network packet arrives, compares said network packet data against said policy specification file and responsive to said comparison assigns associated policy dispositions and level of severity to said network events contained in said network packet data,

Accordingly, in view of the above, neither prior art of reference alone or in combination teach, disclose, suggest, or motivate all claim limitations of Claims 1 and 13. Therefore, Claims 1 and 13 and the respective dependent claims, are in condition for allowance. Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

(b) Claim 33 (and 25)

Applicant has amended Claim 33 (25) to incorporate the policy monitor component of Claim 1 (13). Therefore, in view of the amendment and in view of the above, neither prior art of reference alone or in combination teach, disclose, suggest, or motivate all claim limitations of Claims 33 and 25. Therefore, Claims 33 and 25 and the respective dependent claims, are in condition for allowance. Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

4. It should be appreciated that Applicant has elected to amend the Claims solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent Business Goals, 65 Fed. Reg. 54603 (9/8/00). In making such amendment, Applicant has not and does not in any way narrow the scope of protection to which Applicant considers the invention herein to be entitled. Rather, Applicant reserves Applicant's right to pursue such protection at a later point in time and merely seeks to pursue protection for the subject matter presented in this submission.

CONCLUSION

Based on the foregoing, Applicant considers the present invention to be distinguished from the art of record. Accordingly, Applicant earnestly solicits the Examiner's withdrawal of the rejections raised in the above referenced Office Action, such that a Notice of Allowance is forwarded to Applicant, and the present application is therefore allowed to issue as a United States patent. The Examiner is invited to call (650) 474-8400 to discuss the response.

Respectfully Submitted,

Julia A. Thomas

Julia A. Thomas
Reg. No. 52,283

Customer No. 22862